

other organization shall deny the employee access to classified information and submit a report to the CSA. The SF-312 must be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date. The individual shall also be given a security orientation briefing in accordance with §95.33 of this chapter. Records of access authorization grant and renewal notification must be maintained by the licensee or other organization for three years after the access authorization has been terminated by the CSA. This information may also be furnished to other representatives of the Commission, to licensees, contractors, or other Federal agencies. Notifications of access authorization will not be given in writing to the affected individual except:

(a) In those cases in which the determination was made as a result of a Personnel Security Hearing or by Personnel Security Review Examiners; or

(b) When the individual also is the official designated by the licensee or other organization to whom written NRC notifications are forwarded.

[62 FR 17688, Apr. 11, 1997]

**§ 25.25 Cancellation of requests for access authorization.**

When a request for an individual's access authorization or renewal of access authorization is withdrawn or canceled, the requestor shall notify the CSA immediately by telephone so that the full field investigation, National Agency Check with Credit Investigation, or other personnel security action may be discontinued. The requestor shall identify the full name and date of birth of the individual, the date of request, and the type of access authorization or access authorization renewal requested. The requestor shall confirm each telephone notification promptly in writing.

[62 FR 17689, Apr. 11, 1997]

**§ 25.27 Reopening of cases in which requests for access authorizations are canceled.**

(a) In conjunction with a new request for access authorization (NRC Form 237 or CSA equivalent) for individuals whose cases were previously canceled,

new fingerprint cards (FD-257) in duplicate and a new Security Acknowledgment (NRC Form 176), or CSA equivalent, must be furnished to the CSA along with the request.

(b) Additionally, if 90 days or more have elapsed since the date of the last Questionnaire for Sensitive Positions (SF-86), or CSA equivalent, the individual must complete a personnel security packet (see §25.17(d)). The CSA, based on investigative or other needs, may require a complete personnel security packet in other cases as well. A fee, equal to the amount paid for an initial request, will be charged only if a new or updating investigation by the NRC is required.

[62 FR 17689, Apr. 11, 1997]

**§ 25.29 Reinstatement of access authorization.**

(a) An access authorization can be reinstated provided that:

(1) No more than 24 months has lapsed since the date of termination of the clearance;

(2) There has been no break in employment with the employer since the date of termination of the clearance;

(3) There is no known adverse information;

(4) The most recent investigation must not exceed 5 years (Top Secret, Q) or 10 years (Secret, L); and

(5) The most recent investigation must meet or exceed the scope of the investigation required for the level of access authorization that is to be reinstated or granted.

(b) An access authorization can be reinstated at the same, or lower, level by submission of a CSA-designated form to the CSA. The employee may not have access to classified information until receipt of written confirmation of reinstatement and an up-to-date personnel security packet will be furnished with the request for reinstatement of an access authorization. A new Security Acknowledgement will be obtained in all cases. Where personnel security packets are not required, a request for reinstatement must state the level of access authorization to be reinstated and the full name and date of birth of the individual to establish positive identification. A fee, equal to the amount paid for an initial request,

will be charged only if a new or updating investigation by the NRC is required.

[62 FR 17689, Apr. 11, 1997]

**§25.31 Extensions and transfers of access authorizations.**

(a) The NRC Division of Security may, on request, extend the authorization of an individual who possesses an access authorization in connection with a particular employer or activity, to permit access to classified information in connection with an assignment with another employer or activity.

(b) The NRC Division of Security may, on request, transfer an access authorization when an individual's access authorization under one employer or activity is terminated, simultaneously with the individual being granted access authorization for another employer or activity.

(c) Requests for extension or transfer of access authorization must state the full name of the person, his date of birth and level of access authorization. The Director, Division of Security, may require a new personnel security packet (see §25.17(c)) to be completed by the applicant. A fee, equal to the amount paid for an initial request, will be charged only if a new or updating investigation by the NRC is required.

(d) The date of an extension or transfer of access authorization may not be used to determine when a request for renewal of access authorization is required. Access authorization renewal requests must be timely submitted, in accordance with §25.21(c).

[45 FR 14481, Mar. 5, 1980, as amended at 48 FR 24320, June 1, 1983; 57 FR 3721, Jan. 31, 1992; 62 FR 17689, Apr. 11, 1997]

**§25.33 Termination of access authorizations.**

(a) Access authorizations will be terminated when:

(1) Access authorization is no longer required;

(2) An individual is separated from employment or the activity for which he obtained an access authorization for a period of 90 days or more; or

(3) An individual, pursuant to 10 CFR part 10 or other CSA approved adjudicatory standards, is no longer eligible for access authorization.

(b) A representative of the licensee or other organization that employs the individual whose access authorization will be terminated shall immediately notify the CSA when the circumstances noted in paragraphs (a)(1) or (a)(2) of this section exist; inform the individual that his access authorization is being terminated, and the reason; and that he will be considered for reinstatement of access authorization if he resumes work requiring it.

(c) When an access authorization is to be terminated, a representative of the licensee or other organization shall conduct a security termination briefing of the individual involved, explain the Security Termination Statement (NRC Form 136 or CSA approved form) and have the individual complete the form. The representative shall promptly forward the original copy of the completed Security Termination Statement to CSA.

[62 FR 17689, Apr. 11, 1997]

CLASSIFIED VISITS

**§25.35 Classified visits.**

(a) The number of classified visits must be held to a minimum. The licensee, certificate holder, or other facility shall determine that the visit is necessary and that the purpose of the visit cannot be achieved without access to, or disclosure of, classified information. All classified visits require advanced notification to, and approval of, the organization to be visited. In urgent cases, visit information may be furnished by telephone and confirmed in writing.

(b) Representatives of the Federal Government, when acting in their official capacities as inspectors, investigators, or auditors, may visit a licensee, certificate holder or other's facility without furnishing advanced notification, provided these representatives present appropriate government credentials upon arrival. Normally, however, Federal representatives will provide advanced notification in the form of an NRC Form 277, "Request for Visit or Access Approval," with the "need-to-know" certified by the appropriate NRC office exercising licensing or regulatory authority and verification of